Title: SHHHHHH! It’s a Secret

Link to Outcomes:

- **Patterns and Relationships** Students will discover the need for a common understanding of symbolic representation and the many ways symbols can be disguised using codes and mathematical processes.

- **Cooperation** Students will operate in pairs and teams of four to decipher and encipher information.

- **Connections** Students will understand how mathematics is used to encode and decode messages.

- **Technology** Students will use the TI-82 graphics calculator to formulate and manipulate matrix operations for encoding and decoding messages.

- **Problem Solving** Students will solve several different encrypting processes and will work together to formulate a process for encrypting their own information.

- **Algebra** Students will use matrices to encode and decode messages.

- **Writing** Students will individually write about the history and processes used in creating and reading ciphers.

Brief Overview:

Understanding symbols has been an important factor in human history. The symbols enhance understanding, but without a key for unlocking the message held within the symbols, the information is useless.

Allowing only a select group of people to have information is an important part of the world of business, nations, and individuals. Each of us has information which is important to us and would pose a threat to our security if it were public knowledge. Social security numbers, pin codes, bank accounts, personal health information, etc. are essential in our personal world but in the hands of someone else, may be threatening. In business coding messages is important so that only those who purchase a service such as HBO may use the service, and the messages are not pirated by those who do not pay for the access.

In the international arena, coding of secure information has moved from fairly simple methods used in the Civil and Revolutionary Wars to the highly complex coding done today with super computers. Mathematics has played an integral part in the development of the programs used in the encoding and decoding processes.

The ciphering and deciphering of codes is termed cryptography and cryptanalysis. These words are derived from the Greek, KRYPTOS (meaning hidden), and LOGOS (meaning speech).

In this lesson, students will gain an understanding of the history and a few of the methods which can be used to hide messages.

Grade/Level:

Algebra I, Geometry, Algebra II. The complexity of the lesson can be changed by using larger matrices and increasing the operations performed. The lesson also could be used for Pre-Algebra, if only the first lesson is used.

Duration:

The unit is composed of two lessons which are designed to run on consecutive days for 45 minute classes.

Prerequisite Knowledge:

The student must have mastered basic matrix knowledge and know how to use the TI-82 to manipulate matrices. The lesson can be simplified to basic Pre-Algebra usage by only using the activities from Lesson 1.

Objectives:

- The students will gain an insight into the history of cryptology and learn how to use several different methods to encode and decode messages.
- Students will understand the role which mathematics plays in enciphering and deciphering codes.

Materials/Resources/Printed Materials:

Each student will need the use of a TI-82 calculator and 3-3x5 index cards. Each pair will need a copy of the lesson sheet. Each group will also need a pair of scissors.

Development/Procedures:

Students should be teamed in groups of four which are subdivided into pairs.

Lesson 1: Teacher's Guide

The teacher will lecture for five minutes on the role of symbols in our culture and mathematics and how messages may be scrambled or coded using different methods. The students also may discuss who would want to code messages and why this is becoming more important in the world.

Students will form groups of four which are sub-divided into pairs. They will receive the first worksheet from their teacher and in pairs will work to find solutions. In Part II, students will work in their groups of four to devise a new code and encrypt their own messages into code. Then groups will exchange cards and work to decode the messages.

Lesson 2: Teacher's Guide

Allocate the first ten minutes of class to follow up on yesterday's assignment. Ask volunteers from some of the groups to share their experiences. Make an effort to ask them to talk about the methods of attack, frustration, success, and the value of having a group versus working as an individual, while decoding.

For Lesson 2, students should work in groups of four. Give each student a copy of the instruction on the Hill Cipher. Students should work through the example in their groups. As they finish the sample message, students should pick up the next worksheet. The groups should work for the rest of the period to decipher a message which is encoded using the Hill Method.

Extension:

The teacher can make a research assignment for each group to write a report on who uses codes and why they are such an important topic.

Evaluation:

The teacher can use a checklist to evaluate the students in Parts I and II of Lesson 1. The teacher can use the same checklist to evaluate group progress and note successes in Lesson 2.

Authors:

Hazel H. Orth
Langley High School
Fairfax County

Sandra W. Williamson
Stratford Academy
Macon, Georgia

REVIEW OF MATRICES

Preliminary Lesson To Teaching Encoding

The activity should be done in pairs using notes.

$$\text{Given matrix } [A] = \begin{bmatrix} 3 & -2 \\ 5 & 7 \end{bmatrix} \text{ and } [B] = \begin{bmatrix} 6 & 5 \\ 3 & 0 \end{bmatrix}$$

Find each of the following using a graphics calculator. Simplify each.

1. $[A] + [B]$

2. $3[A] - 2[B]$

3. $[A^{-1}$

4. $[A]^{-1}[A]$

5. $[A]^{-1}[B]$

6. $[B]^{-1}[A]$

7. What is the result to problem 4 called?

LESSON 1

BE A CRYPTANALYST

NAME________________________________ DATE_______________

The Caesar Cipher was invented by Julius Caesar over two thousand years ago. It involves using a shift in the positions of the letters of the alphabet forward three letters to create an new alphabet and was used to send secret messages.

Standard	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Caesar	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Cipher “ PBKA LRQ CLO MFWWX ”

Plain text “ SEND OUT FOR PIZZA ”

DIRECTIONS:

Part I

Students should work in pairs to solve the following problem:

This question was encoded using a Caesar-type shift, but not the same shift as in the example above. Decipher the question, and answer it. (Extra credit if your answer is in cipher text.)
* **Hint**: One of the words is “SECRET.”

SQD OEK TUSETU JXYI IUSHUJ CUIIQWU?

Question in plain text_____________________________________

Answer in plain text____

Answer in cipher text____

Raise your hand when you have finished so that the teacher can see if your answers are correct. While you are waiting for the other pair in your group to finish, each of you can experiment with variations of the Caesar cipher to make a new code.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

____

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Part II

In your groups of four, discuss the variations which are possible and devise a new way to use the letters of the alphabet to make a more complex code. You may wish to cut out the alphabet strips at the bottom of the previous page in order to facilitate the process. Decide upon a message which is between 15 and 30 letters long and encrypt that message using your new cipher. Write the directions for your cipher on one 3x5 card, and then write your encrypted message "CLEARLY" on the second card. You will have 10 minutes to complete this task.

When the teacher calls time, each group will exchange its encrypted message with another group. Each group then will work to decipher the code and write the plaintext message on the back of the card and a description of the cipher method used. If the group cannot decipher the message, they may then work on it for homework.

LESSON 2

Name________________________________ Date____________

HILL CODES

One method of encoding is called the Hill cipher which was published by Lester S. Hill in the "Atlantic Monthly" in 1929. The method used matrices to encode the message. Matrix multiplication converted the information into a new matrix which was not decipherable to those encountering it. If the matrix used were not known, the cryptanalyst had to go through all possible combinations of numbers to find the correct matrix. The larger the cipher matrix, the more difficult it is to find the precise array of numbers which will allow the cryptanalyst to decipher the message. Matrix operations also can be used to make the code even more difficult to break.

Guidelines for Encoding and Decoding Using Hill's Method

To Encode

Step 1 Arrange the letters of your message in matrix form. We will use a 2x2 matrix.

Message: MEET ME AT THE LIBRARY

ME ME TH IB RY
ET AT EL RA QQ*

*Note: Use dummy letters to complete the matrix.

Step 2 Substitute a number for each letter using the chart below.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

$$\begin{bmatrix} 13 & 5 \\ 5 & 20 \end{bmatrix} \quad \begin{bmatrix} 13 & 5 \\ 1 & 20 \end{bmatrix} \quad \begin{bmatrix} 20 & 8 \\ 5 & 12 \end{bmatrix} \quad \begin{bmatrix} 9 & 2 \\ 18 & 1 \end{bmatrix} \quad \begin{bmatrix} 18 & 25 \\ 17 & 17 \end{bmatrix}$$

Step 3 Select a cipher matrix.

Let's use $\begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix}$

Step 4 Multiply each matrix found in step 2 by the cipher matrix.

For example:

$$\begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} * \begin{bmatrix} 13 & 5 \\ 5 & 20 \end{bmatrix} = \begin{bmatrix} 31 & 30 \\ 80 & 85 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} * \begin{bmatrix} 13 & 5 \\ 1 & 20 \end{bmatrix} = \begin{bmatrix} 27 & 30 \\ 68 & 85 \end{bmatrix}$$

Continue with this pattern for each of the message matrices.

Note: Matrix multiplication is NOT commutative.

The encoded message matrices are:

$$\begin{bmatrix} 31 & 30 \\ 80 & 85 \end{bmatrix} \quad \begin{bmatrix} 27 & 30 \\ 68 & 85 \end{bmatrix} \quad \begin{bmatrix} 45 & 28 \\ 115 & 76 \end{bmatrix} \quad \begin{bmatrix} 36 & 5 \\ 99 & 13 \end{bmatrix} \quad \begin{bmatrix} 53 & 67 \\ 141 & 176 \end{bmatrix}$$

TO DECODE

Step 1 Find the inverse of the cipher matrix.

$$\text{cipher matrix} \quad \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \qquad \text{inverse} \quad \begin{bmatrix} 3 & -1 \\ -5 & 3 \end{bmatrix}$$

Step 2 Multiply ON THE LEFT by the inverse.

$$\begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix} * \begin{bmatrix} 31 & 30 \\ 80 & 85 \end{bmatrix} = \begin{bmatrix} 13 & 5 \\ 5 & 20 \end{bmatrix}$$

Continue until all matrices have been multiplied. This retrieves the original ciphers which can be matched with their corresponding letters to reveal the message.

13	5	5	20	…
M	E	E	T	…

BE A CRYPTANALYST

Name_________________________________ Date___________

Here's a message which has ben encoded using the Hill Method.

Message in cipher text:

$$\begin{bmatrix} 50 & 60 \\ 2 & 15 \end{bmatrix} \quad \begin{bmatrix} 62 & 30 \\ 33 & 25 \end{bmatrix} \quad \begin{bmatrix} 60 & 48 \\ -6 & 19 \end{bmatrix} \quad \begin{bmatrix} 69 & 96 \\ 12 & 17 \end{bmatrix}$$

Note: The cipher matrix used to produce this message is $\begin{bmatrix} 3 & 1 \\ -1 & 2 \end{bmatrix}$

Write the inverse of the cipher matrix. ____________________

Show all the work which decodes the message.

Write the message in plain text.

____

LESSON 1 STUDENT WORKSHEET
ANSWERS

Question in plain text: CAN YOU DECODE THIS SECRET MESSAGE?

Answer in plain text: YES

Answer in cipher text: OUI

LESSON 2 STUDENT WORKSHEET
ANSWERS

Message in plain text: NO HOMEWORK FOR YOU